The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
1/10/2017

SUBJECT:
Multiple Vulnerabilities in Adobe Acrobat and Adobe Reader Could Allow for Code Execution (APSB17-01)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader, the most severe of which could allow for code execution. Adobe Acrobat and Reader allow a user to view, create, manipulate, print and manage files in Portable Document Format (PDF). Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Adobe Acrobat DC versions 15.020.20042 and prior for Windows and Macintosh
- Acrobat Reader DC versions 15.020.20042 and prior for Windows and Macintosh
- Acrobat DC versions 15.006.3044 and prior for Windows and Macintosh
- Adobe Acrobat Reader DC versions 15.006.3044 and prior for Windows and Macintosh
- Adobe Acrobat XI versions 11.0.18 and prior for Windows and Macintosh
- Adobe Reader XI versions 11.0.18 and prior for Windows and Macintosh

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader, the most severe of which could allow for code execution. The vulnerabilities are as follows:

- One type confusion vulnerability that could lead to code execution (CVE-2017-2962).

- Seven use-after-free vulnerabilities that could lead to code execution (CVE-2017-2950, CVE-2017-2951, CVE-2017-2955, CVE-2017-2956, CVE-2017-2957, CVE-2017-2958, CVE-2017-2961).
- Six heap buffer overflow vulnerabilities that could lead to code execution (CVE-2017-2942, CVE-2017-2945, CVE-2017-2946, CVE-2017-2949, CVE-2017-2959, CVE-2017-2966).
- Two buffer overflow vulnerabilities that could lead to code execution (CVE-2017-2948, CVE-2017-2952).
- Twelve memory corruption vulnerabilities that could lead to code execution (CVE-2017-2939, CVE-2017-2940, CVE-2017-2941, CVE-2017-2943, CVE-2017-2944, CVE-2017-2953, CVE-2017-2954, CVE-2017-2960, CVE-2017-2963, CVE-2017-2964, CVE-2017-2965, CVE-2017-2967).
- One security bypass vulnerability (CVE-2017-2947).

Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Adobe:
https://helpx.adobe.com/security/products/acrobat/apsb17-01.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2939
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2940
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2941
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2942
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2943
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2944
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2945
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2946
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2947
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2948
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2949
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2950
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2951
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2952
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2953
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2954

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2955
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2956
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2957
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2958
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2959
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2960
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2961
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2962
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2963
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2964
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2965
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2966
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2967

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/